



TITLE:

有理数体上定義される楕円曲線に
付随する canonical power series について(代数的整数論とその周辺)

AUTHOR(S):

山本, 芳彦

CITATION:

山本, 芳彦. 有理数体上定義される楕円曲線に付随する canonical power series について(代数的整数論とその周辺). 数理解析研究所講究録 1998, 1026: 204-211

ISSUE DATE:

1998-02

URL:

<http://hdl.handle.net/2433/61754>

RIGHT:

有理数体上定義される楕円曲線に付随する canonical power series について

大阪大学理学研究科 山本芳彦
Yoshihiko YAMAMOTO, Osaka University

1 Canonical parameter と canonical series

C を有理数体上定義された楕円曲線で, Weierstrass form の定義方程式

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \quad (a_i \in \mathbb{Z}) \quad (1)$$

で与えられているものとする. 方程式 (1) の判別式を $\Delta = \Delta(C)$ とする.

(議論を簡単にするため, 以後, (1) は minimal model であると仮定し, その判別式を Δ , 導手を N とする.)

通例のように, C に無限遠点 O を零元とする abel 多様体の構造を入れる. O における局所変数 t を適当に選ぶと, X, Y は C 上の有理関数として, 次の形の形式的べき級数としてあらわされる.

$$X = t^{-2} + x_{-1}t^{-1} + x_0 + x_1t + x_2t^2 + \cdots \quad (x_i \in \mathbb{Q}) \quad (2)$$

$$Y = t^{-3} + y_{-2}t^{-2} + y_{-1}t^{-1} + y_0 + y_1t + \cdots \quad (y_j \in \mathbb{Q}) \quad (3)$$

X, Y が方程式 (1) を満たすことより 係数 x_i, y_j の間には次の関係が成り立つことがわかる:

$$\begin{cases} 3x_{-1} - 2y_{-2} &= a_1 \\ 3x_0 - 2y_{-1} &= -a_2 + a_1x_{-1} - 3x_{-1}^2 + a_1y_{-2} + y_{-2}^2 \\ 3x_1 - 2y_0 &= a_3 - 2a_2x_{-1} - x_{-1}^3 + a_1x_0 - 6x_{-1}x_0 \\ &\quad + a_1x_{-1}y_{-2} + a_1y_{-1} + 2y_{-2}y_{-1} \\ 3x_2 - 2y_1 &= \cdots \end{cases}$$

一般に, $n \geq -1$ に対して次が成り立つ.

$$3x_n - 2y_{n-1} = A_n \quad (4)$$

ここで, A_n は $a_1, a_2, a_3, a_4, a_6, x_{-1}, \dots, x_{n-1}$, および y_{-2}, \dots, y_{n-2} に関する有理整数係数の多項式である.

とくに, t として

$$t = \frac{X}{Y} \quad (5)$$

をとるとき,

$$x_n = y_{n-1} \quad (n \geq -2)$$

が成り立ち, X, Y の t -展開係数は (4) により順次に定まる. さらに, そのとき, すべての係数 $x_{-1}, x_0, \dots, y_{-2}, y_{-1}, \dots$ は有理整数である.

このように, X, Y のすべての係数 $x_i (i \geq -1), y_j (j \geq -2)$ が有理整数であるとき, 局所変数 t を (C の O における) **integral parameter** とよぶことにする.

t を **integral parameter** とするとき, 形式的べき級数

$$t' = \phi(t) = t + r_2 t^2 + r_3 t^3 + \dots \quad (r_i \in \mathbb{Z}) \quad (6)$$

で与えられる局所変数 t' も **integral parameter** である. 従って, C には無数の **integral parameter** が存在する.

C 上の有理関数 X, Y に対して

$$\omega = \frac{-dX}{2Y + a_1 X + a_3}$$

は C の O でない 1 つの正則微分を与える. O における局所変数 t に対して, X, Y が (2), (3) とべき級数展開されるとき,

$$\Omega_t = \frac{-t}{2Y + a_1 X + a_3} \frac{dX}{dt} = t + c_2 t^2 + c_3 t^3 + \dots \quad (c_i \in \mathbb{Q}) \quad (7)$$

とおく. とくに t が **integral** のとき, c_2, c_3, \dots は有理整数である.

C の **zeta 関数**を

$$L_C(s) = \prod_p L_{C,p}(s) = \sum_{n=1}^{\infty} a_n n^{-s} \quad (8)$$

$$L_{C,p}(s) = \begin{cases} (1 - a_p p^{-s} + p^{1-2s})^{-1} & \text{if } p \nmid \Delta \\ (1 - a_p p^{-s})^{-1} & \text{if } p \mid \Delta \end{cases}$$

とするとき,

$$\Omega_t \frac{dt}{t} = \omega$$

であることより, **integral parameter** t に関して次の命題が成り立つことが知られている.

Proposition 1.1 p を $p \nmid \Delta$ を満たす素数とするとき, $c_p \equiv a_p \pmod{p}$.

$p \nmid \Delta$ のとき, $L_{C,p}(s)$ に関する **Riemann 予想** $|a_p| \leq 2\sqrt{p}$ が成り立つ. また, $p \geq 17$ ならば, $2\sqrt{p} \leq \frac{1}{2}p$ だから, 上の命題において, 次がいえる.

$$p \nmid \Delta, p \geq 17, |c_p| \leq \frac{p}{2} \Rightarrow c_p = a_p$$

Definition 1.1 C の integral parameter t について

$$c_n = a_n \quad (n \geq 1)$$

が成り立つとき, t を C の **canonical parameter** という.

また, **canonical parameter** t による X, Y の形式的べき級数展開 (2), (3) を C の **canonical series** といい, これらをまとめて, C の **canonical system** とよぶ.

例 1.1 楕円曲線

$$C_1: Y^2 + Y = X^3 - X^2 - 10X - 20 \quad \Delta(C) = -11^5$$

を考える. この曲線は合同部分群 $\Gamma_0(11)$ に関する保型関数体の \mathbb{Q} 上の一つのモデルを与えている. このとき, X, Y は複素上半平面の変数 z の保型関数として, $q = \exp(2\pi iz)$ により次のように整数係数で展開される.

$$X = \frac{1}{q^2} + \frac{2}{q} + 4 + 5q + 8q^2 + q^3 + 7q^4 - 11q^5 + 10q^6 - 12q^7 - 18q^8 - 22q^9 + 26q^{10} - \dots \quad (9)$$

$$Y = \frac{1}{q^3} + \frac{3}{q^2} + \frac{7}{q} + 12 + 17q + 26q^2 + 19q^3 + 37q^4 - 15q^5 - 16q^6 - 67q^7 - 6q^8 - 144q^9 + \dots \quad (10)$$

また, $\omega = 2\pi i \Omega_q dz$ より,

$$\Omega_q = q - 2q - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} + \dots$$

は $\Gamma_0(11)$ に関する weight 2 の newform であり, この newform に Melin 変換により, 対応する Dirichlet 級数

$$\begin{aligned} & 1 - \frac{2}{2^s} - \frac{1}{3^s} + \frac{2}{4^s} + \frac{1}{5^s} + \frac{2}{6^s} - \frac{2}{7^s} - \frac{2}{9^s} - \frac{2}{10^s} + \frac{1}{11^s} - \frac{2}{12^s} + \frac{4}{13^s} \dots \\ &= \left(1 + \frac{2}{2^s} + \frac{2}{2^{2s}}\right)^{-1} \left(1 - \frac{1}{3^s} + \frac{3}{3^{2s}}\right)^{-1} \left(1 - \frac{1}{5^s} + \frac{5}{5^{2s}}\right)^{-1} \left(1 + \frac{2}{7^s} + \frac{7}{7^{2s}}\right)^{-1} \\ & \quad \times \left(1 - \frac{1}{11^s}\right)^{-1} \left(1 - \frac{4}{13^s} + \frac{13}{13^{2s}}\right)^{-1} \dots \end{aligned}$$

は C_1 の zeta 関数となることが知られている (Eichler- Shimura). このことから, 上の q 展開 (9), (10) は C_1 の **canonical system** を与えることがわかる.

2 Canonical system の存在と構成

楕円曲線 C の一つの integral parameter t をとり, $X = X(t)$, $Y = Y(t)$ は t により, (2), (3) のように展開されているとする. このとき, (7) により, Ω_t も整数係数である. ここで,

$$h(t) = t + \frac{c_2}{2}t^2 + \frac{c_3}{3}t^3 + \cdots = \int \Omega_t \frac{dt}{t} \quad (11)$$

とおくとき, C の \mathbb{Z} 上の formal group としての構造 $C(u, v) = C_t(u, v)$ が次のようにして定まる (T.Honda).

$$C_t(u, v) = h^{-1}(h(u) + h(v)) = u + v + \cdots \in \mathbb{Z}[[u, v]]$$

C の二つの integral parameter t と t' が, 整係数の変数変換 (6) で移りあうとき, $t' = \phi(t)$ で定まる formal group を $C' = C_{t'}$ とすると, 次が成り立つ:

$$\phi(C(u, v)) = C'(\phi(u), \phi(v))$$

このとき, $\phi(t)$ を formal group C より formal group C' への 強同型 であるという.

C の zeta 関数 (8) に対応する整級数 $g(q)$

$$g(q) = \sum_{n=1}^{\infty} \frac{a_n}{n} q^n \quad (12)$$

で定まる formal group を

$$G(u, v) = g^{-1}(g(u) + g(v))$$

とする. このとき,

Theorem 2.1 (T.Honda) Formal group $C_t(u, v)$ より formal group $G(u, v)$ への強同型が一意に存在する.

この定理より, C の integral parameter t を適当にとれば, 対応する formal group $C_t(u, v)$ は $G(u, v)$ と一致する. よって,

$$c_n = a_n \quad (n \geq 1)$$

従って,

Theorem 2.2 (T.Honda) \mathbb{Q} 上の任意の楕円曲線 C に対して canonical system が存在し一意に定まる.

C の zeta 関数がすでにわかっているときには, canonical system $X(q), Y(q)$ は次のようにして求めることができる.

(7) より

$$-t \frac{dX}{dt} = (t + c_2 t^2 + c_3 t^3 + \cdots)(2Y + a_1 X + a_3)$$

展開係数を比べることにより, $n \geq -1$ に対して, x_n, y_{n-1}, c_{n+3} の間に, 次の関係式が成り立つことがわかる.

$$nx_n + 2y_{n-1} + 2c_{n+3} = B_n \quad (13)$$

ここで, B_n は $a_1, a_3, c_2, \dots, c_{n-1}, x_{-1}, \dots, x_{n-1}$, および, y_{-2}, \dots, y_{n-2} に関する有理整数係数の多項式である.

(4), (13) で, $c_n = a_n$ において, x_n, y_{n-1} に関する連立方程式

$$\begin{cases} 3x_n - 2y_{n-1} = A_n \\ nx_n + 2y_{n-1} = B_n - 2c_{n+3} \end{cases} \quad (14)$$

を, $n = -1, 0, 1, \dots$ と再帰的に解くことにより, $x_n, y_{n-1} (n \geq -1)$ が一意に定まる. このとき, (2), (3) によって C の canonical system が与えられることは明らか.

さらに, C の zeta 関数がわかっていないときにも, 次の定理により canonical system を求める, と同時に, zeta 関数も求めることができる.

Theorem 2.3 C に対して, 次の方程式

$$\begin{cases} 3x_n - 2y_{n-1} = A_n \\ nx_n + 2y_{n-1} + 2c_{n+3} = B_n \end{cases} \quad (15)$$

をみたす有理整数の列 $\{x_n\}_{n \geq -1}$, $\{y_n\}_{n \geq -2}$, $\{c_n\}_{n \geq 2}$ でさらに次の条件 (i), (ii) をみたすものが一意的に定まる.

(i) $(m, n) = 1$ のとき, $c_{mn} = c_m c_n$

(ii) 素数 p に対して,

(a) $|c_p| \leq \frac{1}{2}p$,

とくに, $a_1 \equiv a_3 \equiv 0 \pmod{2}$ ならば $c_2 = 0$

(b) $p \nmid \Delta(C)$ のとき, $c_{p^k} = c_p c_{p^{k-1}} - p c_{p^{k-2}} \quad (k \geq 2)$

(c) $p \mid \Delta(C)$ のとき, $c_{p^k} = c_p^k$

このとき,

$$\begin{cases} X = t^{-2} + x_{-1} t^{-1} + x_0 + x_1 t + x_2 t^2 + \cdots \\ Y = t^{-3} + y_{-2} t^{-2} + y_{-1} t^{-1} + y_0 + y_1 t + \cdots \end{cases} \quad (16)$$

は C の canonical system となり, C の zeta 関数は

$$L_C(s) = \sum_{n=1}^{\infty} c_n n^{-s} \quad (17)$$

で与えられる.

定理の条件を満たす解が存在することは, canonical system の存在より明らかである. また, 連立不定方程式 (15) を $\{x_n, y_{n-1}\}$ に関する連立方程式と見るとき, その判別式は $2(n+3)$ であることより一意性もいえる.

具体的に, 不定方程式 (15) を $n = -1$ より順に再帰的に求めてみると, $n+3 = p$ が素数でかつ $p \leq 13$ のときには, 条件 (ii) だけでは c_p の値は一意には定まるとは限らないが, 正しい c_p の値以外の場合には, (15) による再帰的アルゴリズムが途中で働かなくなる. このような例外は有限個であるから, 最終的には, アルゴリズムはうまく働き, ただ一つの解を得ることがわかる.

上の定理で与えられたアルゴリズムによると, C の zeta 関数の計算が, 素数 p に関する局所 zeta 関数 $L_{C,p}(s)$ を (p が good または bad の場合とも) 計算することなしに, 不定方程式の解を求めることだけで可能となっている. このことは非常に興味深い.

例 2.1 導手 11 の楕円曲線には同型を除いて 3 個あることが知られている (例えば Cremona). 1 つは例 1.1 の曲線 C_1 であり, 残りの 2 つは下の C_2, C_3 である. それぞれに対する canonical system は次で与えられる. これら 3 個の曲線は互いに degree 5 の isogeny で結ばれているので, それぞれの zeta 関数は C_1 の zeta 関数と一致する.

(i) 楕円曲線

$$C_2 : Y^2 + Y = X^3 - X^2 - 7820X - 263580 \quad \Delta = -11, N = 11$$

の canonical system:

$$\begin{aligned} X &= q^{-2} + 2q^{-1} + 4 + 5q + 1570q^2 - 3123q^3 + 38551q^4 - 149501q^5 \\ &\quad + 992122q^6 - 4816670q^7 + 26533203q^8 - 135361908q^9 + \dots \\ Y &= q^{-3} + 3q^{-2} + 7q^{-1} + 12 - 1545q + 1588q^2 - 75507q^3 + 227396q^4 \\ &\quad - 2598721q^5 + 12040848q^6 - 85035369q^7 + 456222970q^8 + \dots \end{aligned}$$

(ii) 楕円曲線

$$C_3 : Y^2 + Y = X^3 - X^2 \quad \Delta = -11, N = 11$$

の canonical system :

$$X = q^{-2} + 2q^{-1} + 4 + 5q + 6q^2 + 5q^3 + 3q^4 - q^5 - 6q^6 - 10q^7 - 11q^8 \\ - 8q^9 + 11q^{11} + 22q^{12} + 28q^{13} + \dots$$

$$Y = q^{-3} + 3q^{-2} + 7q^{-1} + 12 + 19q + 24q^2 + 25q^3 + 18q^4 + 3q^5 - 20q^6 \\ - 45q^7 - 62q^8 - 60q^9 - 31q^{10} + 26q^{11} + 100q^{12} + \dots$$

3 Taniyama-Shimura 予想と canonical system

楕円曲線 C の canonical system $X = X(t), Y = Y(t)$ に対して, $t = q = \exp(2\pi iz)$ とおくと, X, Y は z の関数となる. $\omega = 2\pi i \Omega_q dz$ より Ω_q は zeta 関数の係数を用いて

$$\Omega_q = q + c_2 q^2 + c_3 q^3 + c_4 q^4 + c_5 q^5 + \dots \quad (18)$$

と q -展開される. 谷山-志村予想によると, C の導手を N とするとき, 上の Ω_q は z の関数として, $\Gamma_0(N)$ に関する weight 2 の cusp form になる. このとき, X, Y は z の関数として modular 関数になり, canonical series はその q -展開を与えている.

実際, 導手 N が square free の場合には, 谷山-志村予想は証明されている (Wiles) ので, C の canonical parameter を $q = \exp(2\pi iz)$ と表すとき, canonical series は modular 関数としての X, Y の q -展開を与えている.

一般に, 谷山-志村予想のもとに, canonical series により C の modular 関数による一意化が与えられることになる.

上のような意味で, 以後, canonical parameter は q と表すことにする.

4 Isogeny と canonical systems

2つの楕円曲線 C, C' の間に isogeny $\lambda : C \rightarrow C'$ があるとき, C の canonical series $X(q), Y(q)$ の λ による像は C' の canonical series $X'(q), Y'(q)$ により次のように表される:

$$\lambda(X, Y) = [d_\lambda](X'(q), Y'(q)) \quad (d_\lambda \in \mathbb{Z})$$

右辺は C' の点 (X', Y') の C' の加法に関する d_λ 倍を表している. 従って, isogeny の積に対して次が成り立つ:

$$d_{\lambda\nu} = d_\lambda d_\nu$$

また, λ の dual isogeny を λ^* とすると

$$d_\lambda d_{\lambda^*} = \deg \lambda$$

とくに, $\deg \lambda = p$ (素数) のとき,

$$|d_\lambda| = 1, |d_{\lambda^*}| = p \quad \text{または} \quad |d_\lambda| = p, |d_{\lambda^*}| = 1$$

であることより,

$$|d_\lambda| = 1 \quad \text{のとき,} \quad C \xrightarrow{p} C'$$

と定義することにより, 導手が N の isogeny class の集合は順序集合となる. 多くの場合について実験した結果, これらの順序集合は常に **最大元** をもっている. d_λ および順序関係については, G. Stevens の結果と同じではないかと思われる.

例 4.1 導手 11 の楕円曲線は例 1.1, 例 2.1 で挙げた 3 個で C_1 と C_2 , C_1 と C_3 の間にそれぞれ $\deg 5$ の isogeny $\lambda_{12}, \lambda_{13}$ がある. このとき,

$$|d_{\lambda_{12}}| = 1, |d_{\lambda_{12}^*}| = 5 \quad |d_{\lambda_{13}}| = 5, |d_{\lambda_{13}^*}| = 1$$

従って, 次のような有向グラフを得る.

$$C_3 \xrightarrow{5} C_1 \xrightarrow{5} C_2$$

このとき, C_3 が最大元である.

References

Shimura, G. : On the zeta-functions of the algebraic curves uniformized by certain automorphic functions, J. Math. Soc. of Japan, 13(1961), 175-331.

Honda, T. : On the theory of commutative formal groups, J. Math. Soc. Japan 22(1970), 213-246.

Cremona, J.E. : Algorithms for modular elliptic curves, Cambridge 1992.

Wiles, A. : Modular elliptic curves and Fermat's Last Theorem, Annales of Math. 142(1995), 443-551

Stevens, D. : Stickelberger elements and modular parametrization of elliptic curves, Inv. Math., 98(1989), 75-106